UGate 3200P

Internet Sharing Router

7-Port Switch & 1-Port Print Server

User’s Guide

FCC Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

P/N: 9560D40001

Copyright © 2000. All Rights Reserved.

Document Version: 1.0D

All trademarks and trade names are the properties of their respective owners.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION...1

Features...2
Package Contents 4
Physical Details 4

CHAPTER 2 INSTALLATION...6

Requirements...6
Procedure..6

CHAPTER 3 CONFIGURATION...8

Overview...8
Configuration Program 9

CHAPTER 4 PC CONFIGURATION...11

Overview...11
TCP/IP Settings...11
Internet Access Configuration 14
Printing Setup 15

CHAPTER5 BASIC SETUP 19

Connecting to the UGate-3200P...19
Basic Setup Screen 19

CHAPTER 6 DEVICE ADMINISTRATION..24

Overview...24
Password...24
NAT (Network Address Translation) 25
TFTP...25
ICMP...25

CHAPTER 7 URL FILTER 26

Overview...26
URL Filter Screen 27

CHAPTER 8 ROUTING...28

Overview...28
UGate-3200P Configuration...28
Router Configuration 30
Routing Example 31

CHAPTER 9 STATUS SCREENS 32

WAN Status 32
Access Logs 36
Device/LAN Status...37

CHAPTER 10 ADVANCED INTERNET...39

Overview...39
Advanced Internet Screen 39
Special Applications 40
Virtual Servers 42

DMZ 46

CHAPTER 11 ACCESS CONTROL 48

Overview..48
Security Groups Screen...49
Workstations...51
Administrator Defined Filters...53

CHAPTER 12 DYNAMIC DNS: - GET YOUR OWN DOMAIN...................54

Overview..54
To use Dynamic DNS 54
Examples..56

APPENDIX A TROUBLESHOOTING...62

Overview..62
General Problems...62
Internet Access...63

APPENDIX B TCP/IP CONFIGURATION FOR MACINTOSH® 64

Using the DHCP Server to Assign IP Addresses 64
Manual Assignment of IP Addresses 65

APPENDIX C SPECIFICATIONS 67

Chapter 1

Introduction

This Chapter provides an overview of the UGate-3200P's and capabilities.

Congratulations on the purchase of your new UGate-3200P. The UGate-3200P is a multi-function device providing the following services:

- 7-Port Switch (10/100Mbps)
- Shared Internet access via DSL or Cable modem.
- Network Printer – LAN users can share the printer attached to the UGate-3200P

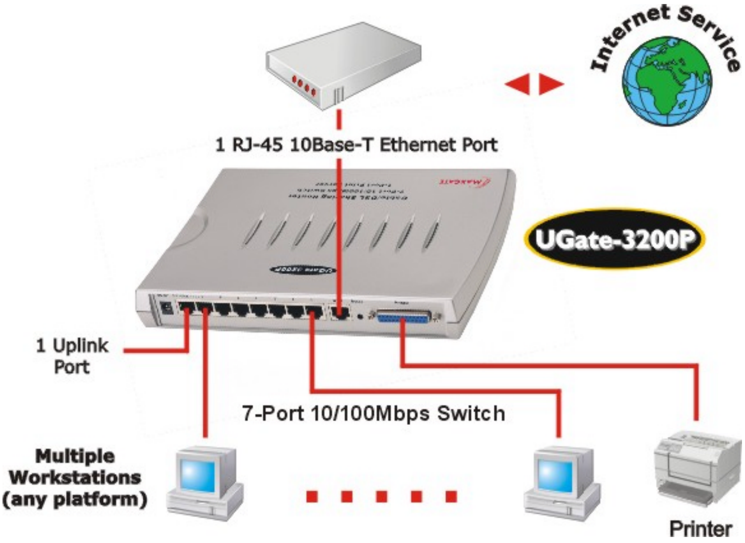


Figure 1:

The UGate-3200P Multi-function Broadband Router can also be used to connect your local LAN to a remote LAN or WAN, instead of providing shared Internet Access.

Features

The UGate-3200P incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

LAN Features

- ***7-Port Switch.*** The UGate-3200P incorporates a 7-port Switch. Both 10BaseT and 100BaseT connections can be used simultaneously.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The UGate-3200P can act as a **DHCP Server** for devices on your local LAN.
- ***Multi Segment LAN Support.*** LANs containing one or more segments are supported, via the UGate-3200P's built-in static routing table. If NAT (Network Address Translation) is disabled, the UGate-3200P will function as a static router.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN can access the Internet through the UGate-3200P, using only one single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***DSL & Cable Modem Support.*** The UGate-3200P has a 10BaseT Ethernet port for connecting DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- ***PPPoE Support.*** Connect to your ISP using PPPoE (PPP over Ethernet), if your ISP uses this method.
- ***Fixed or Dynamic IP Address.*** On the WAN connection, the UGate-3200P supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN for configuration.
- ***Remote Management.*** The UGate-3200P can be managed from a workstation anywhere on the WAN, using a WEB browser.

Advanced Internet Functions

- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***User-Defined Virtual Servers.*** Internet users can access non-standard Internet Servers on your LAN by using this feature.

- ***Special Internet Applications.*** Internet applications such as Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers are supported.

- ***DMZ.*** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet.

Security Features

- ***Configuration Data***. Optional password protection is provided to prevent unauthorized users from modifying the configuration.
- ***Access Control Features***. The LAN Administrator can limit Internet access by individual PCs.
- ***Firewall Protection.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources. (This protection is lost if NAT is disabled.)

Firewall Protection

The firewall protection provided by the UGate-3200P is an intrinsic side effect of NAT (Network Address Translation). All users on the LAN share a single external IP address. From the external viewpoint, there is no network, only a single device.

For internal users, the UGate-3200P acts as a “transparent proxy server”, translating the multiple internal IP addresses into a single external IP address.

For external requests, any attempts to connect to local resources are blocked. The UGate-3200P will not “ reverse translate” from a global IP address to a local IP address.

This type of “natural” firewall provides an impregnable barrier against malicious attacks.

Package Contents

The following items should be included:

- The UGate-3200P Unit
- Power Adapter
- Quick Installation Guide
- Warranty Card
- CD-ROM containing the User's Guide and Print server Driver.

If any of the above items are damaged or missing, please contact your dealer as soon as possible.

Physical Details

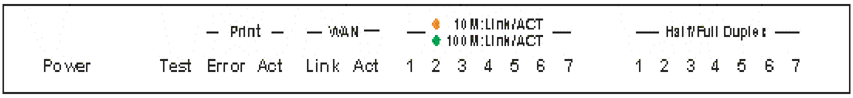


Figure 2: The front panel of the UGate-3200P

LEDs

Power (Green)	ON - power on OFF - no power
Test (Red)	Blinks during start up. ON indicates an error condition.
Print Error (Red)	ON - Printer error detected. OFF - No printer error detected.
Print Act (Green)	• OFF - no connection to printer. • ON - Connection to printer established. • Flashing - Data is being transmitted to the printer.
WAN: Link (Green)	ON - WAN connection is established. OFF - no WAN connection.
WAN: Act (Green)	Flashing - data is being transmitted or received via the WAN port. OFF - no data is being transferred.

LAN: Link/Act (Green/Orange)	There are 7 LEDs - one for each LAN port, and each LED could be OFF, Yellow, or Green. • OFF - No LAN connection on this port. • Orange – 10Mbps link. • Green – 100Mbps link. • This LED flashes when data is being transmitted or received.
LAN: Half/Full Duplex (Green)	ON indicates the LAN connection is using Full Duplex. OFF indicates the LAN connection (if any) is using Half Duplex.

Rear Panel

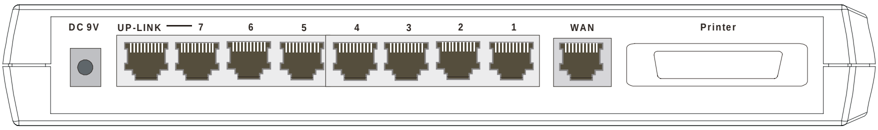


Figure 3: Rear Panel

Power port (9V)	Connect the supplied power adapter here.
Switch ports (10/100Mbps)	Use standard LAN cables (RJ45 connectors) to connect these ports to your PCs. Both 10Mbps and 100Mbps connections can be used simultaneously. **Note:** Use the "Uplink" port only to connect to a normal port on another hub/switch.
WAN port (10Mbps)	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
Reset Button	When pressed and released, the UGate-3200P will reboot (restart). If depressed and held for more than 3 seconds, all data will be cleared, and the factory default values restored.
Printer Port	Standard parallel printer port. If you wish to share a printer, connect it here.

Chapter 2

Installation

2

This Chapter explains how to install the Ugate-3200P.

Requirements

- Ethernet LAN (10/100Mbps) and the TCP/IP protocol.
- For Internet Access, DSL or Cable modem, and an Internet Access account with an ISP.

Procedure

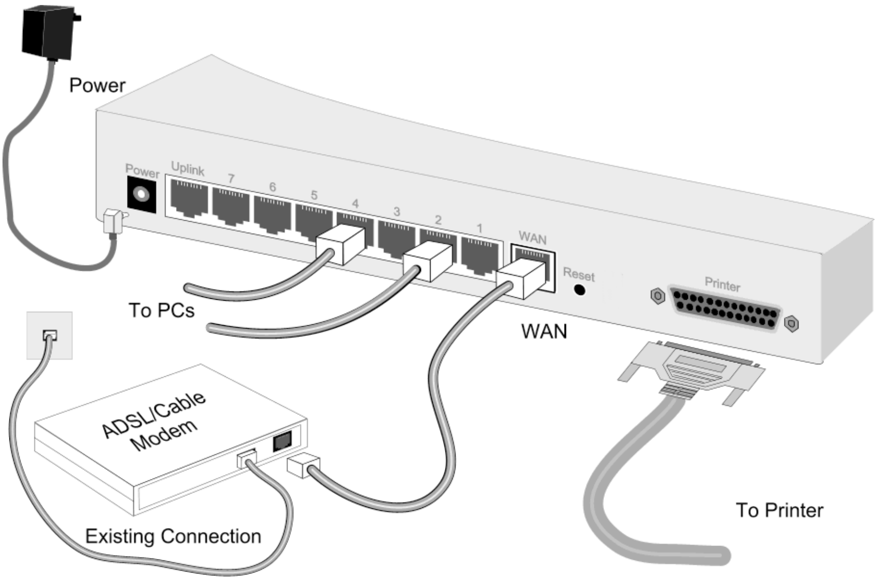


Figure 4 Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the . Ensure the UGate-3200P and the Cable/DSL modem is powered OFF.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switch ports on the UGate-3200P. Both 10Mbps and 100Mbps connections can be used simultaneously.

3. Connect WAN Cable

Connect the DSL or Cable modem to the WAN port on the UGate-3200P. Use the cable supplied with your modem. If no cable was supplied, use a standard LAN cable.

4. Connect the Printer

Use a standard parallel printer cable to connect the printer to the parallel port on the Ugate-3200P.

4. Power Up

Connect the supplied power adapter and power up.

Use only the power adapter provided. Using a different one may cause hardware damage

5. Check the LEDs

When the UGate-3200P is powered On, The Test LED should flash, then turn off. If it stays on, there is a hardware error.

For more information, refer to LEDs in Chapter 1.

Chapter 3

Configuration

This Chapter provides details of the configuration process.

Overview

To make your UGate-3200P operational, only *Basic Setup*, as described in Chapter 5, is required.

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the UGate-3200P you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure the UGate-3200P for basic operation	Chapter 5: Basic Setup
Set a password for the UGate-3200P, disable NAT (Network Address Translation), enable or disable TFTP and ICMP.	Chapter 6: Device Administration
Block site access using the URL Filter function.	Chapter 7: URL Filter
Configure the UGate-3200P and routers for a LAN that has 1 or more routers.	Chapter 8: Routing
Check the UGate-3200P or connection status.	Chapter 9: Status Screens
Use any of the following features: • Special Internet Applications • Virtual Servers • DMZ	Chapter 10: Advanced Internet Features
Limit Internet Access by individual workstations	Chapter 11: Access Control
Provide an easy way for Internet Users to access Servers on your LAN.	Chapter 12: Dynamic DNS:- Get your own Domain Name.

Note! *Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.*

Configuration Program

The UGate-3200P contains a HTTP server. This enables you to connect to it, and configure it, using your Web Browser.

Most Browsers should work, provided they support HTML tables and forms.

Preparation

Before attempting to configure the UGate-3200P, please ensure that:

- Your PC can establish a physical connection to the UGate-3200P. The PC and the UGate-3200P must be connected using the Switch ports on the UGate-3200P, or on the same LAN segment.
- The UGate-3200P must be installed and powered ON.
- If the UGate-3200P's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the UGate-3200P is allocated a new IP Address during configuration.

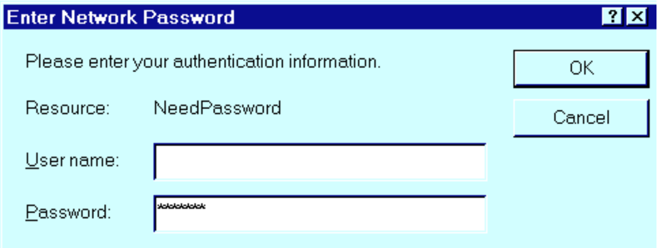
Connecting to the UGate-3200P

To establish a connection from your PC to the device:

1. After installing the UGate-3200P in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the UGate-3200P, as in the following example, which uses the UGate-3200P's default IP Address:

   `HTTP://192.168.0.1`

4. If you have assigned a password to the UGate-3200P you will be prompted for the password, as shown below. (If no password has been set, this dialog will not appear.)



Enter Network Password

Please enter your authentication information.

Resource: NeedPassword

User name:

Password: *******

Figure 5: Password Dialog

- Leave the "User Name" blank.
- Enter the password for this device, if one has been set.

5. You should then see the *Basic Setup* screen. See ***Chapter 5 - Basic Setup*** for details of using this screen.

If you can't connect

If the UGate-3200P does not respond, check the following:

- The UGate-3200P is properly installed, LAN connection is OK, and it is powered ON.
- Ensure that your PC and the UGate-3200P are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the UGate-3200P's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 – PC Configuration* for details on checking your PC’s TCP/IP settings.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, to move from screen to screen.
- On each screen, clicking the "Help" button will display help for that screen.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must “Save” before changing screens or your data will be ignored.

Chapter 4

PC Configuration

This Chapter details the PC Configuration required to work with the UGate-3200P.

Overview

For each PC, the following may to be configured:

- TCP/IP network settings
- Internet Access configuration
- Network printer

This chapter covers Windows system only.

Macintosh users should refer to Appendix B.

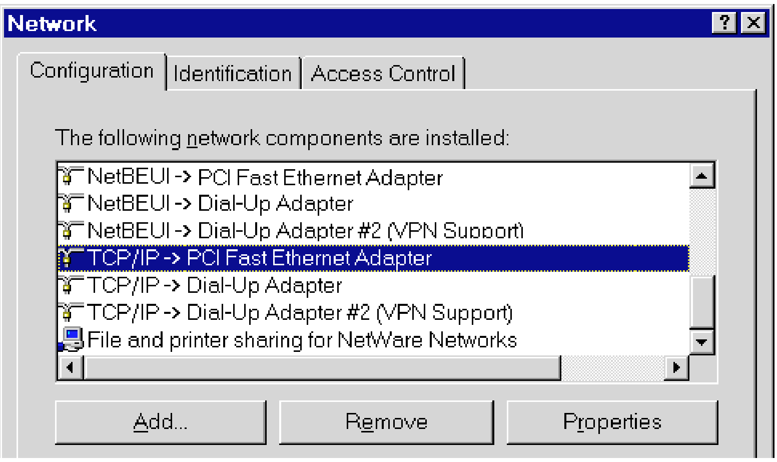
TCP/IP Settings

If using the default UGate-3200P settings, and the default Windows 95/98 TCP/IP settings, no changes need to be made.

- By default, the UGate-3200P will act as a DHCP Server, automatically providing a suitable IP Address to each PC when the PC boots.
- The default Windows 95/98 TCP/IP setting is to act as a DHCP client.

To check your PC's TCP/IP Settings:

1. Select *Control Panel - Network*. You should see a screen like the following:



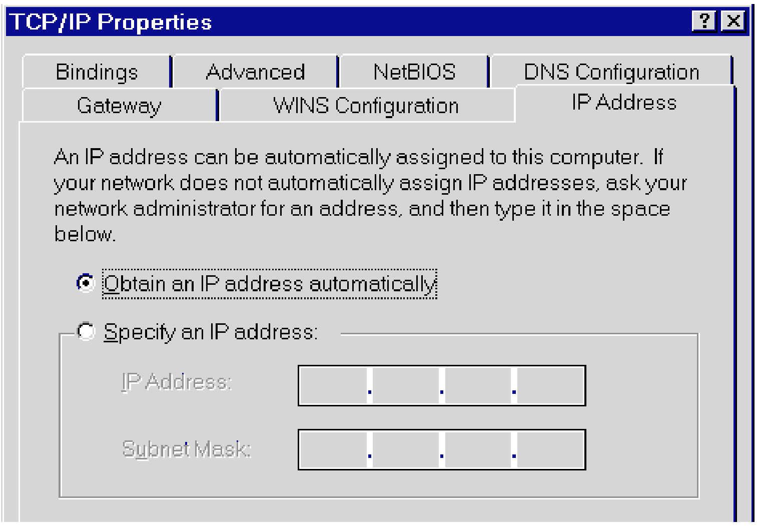
The following network components are installed:

NetBEUI -> PCI Fast Ethernet Adapter
NetBEUI -> Dial-Up Adapter
NetBEUI -> Dial-Up Adapter #2 (VPN Support)
TCP/IP -> PCI Fast Ethernet Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> Dial-Up Adapter #2 (VPN Support)
File and printer sharing for NetWare Networks

Figure 6: Network Configuration

2. Select the *TCP/IP* protocol for your network card.

3. Click on the *Properties* button. You should then see a screen like the following.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Figure 7: IP Address (Win 95/98)

Ensure your TCP/IP settings are correct, as follows:

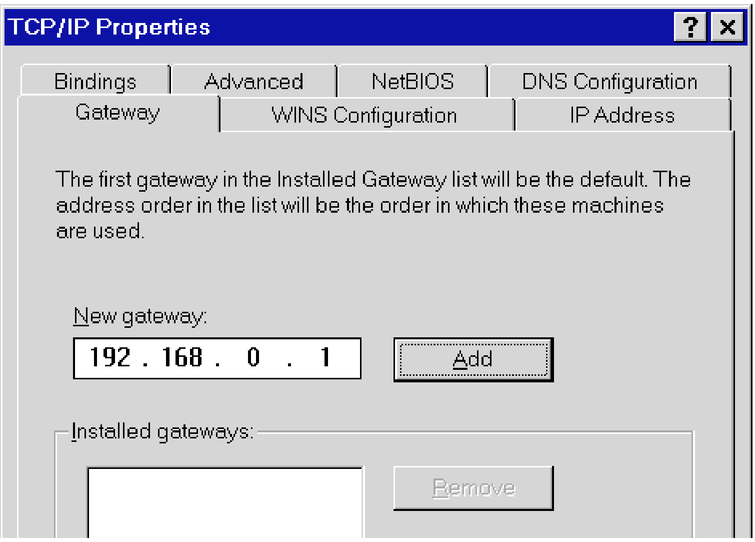
Using DHCP

To use DHCP, select the radio button "***Obtain an IP Address automatically***." This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the UGate-3200P.

Using "Specify an IP Address"

- If your PC is already configured, do NOT change the settings on the IP Address tab shown in Figure 7 above.
- On the *Gateway* tab, set the *Default Gateway Address* to the UGate-3200P's IP address. Your LAN administrator can advise you of the IP Address they assigned to the UGate-3200P.

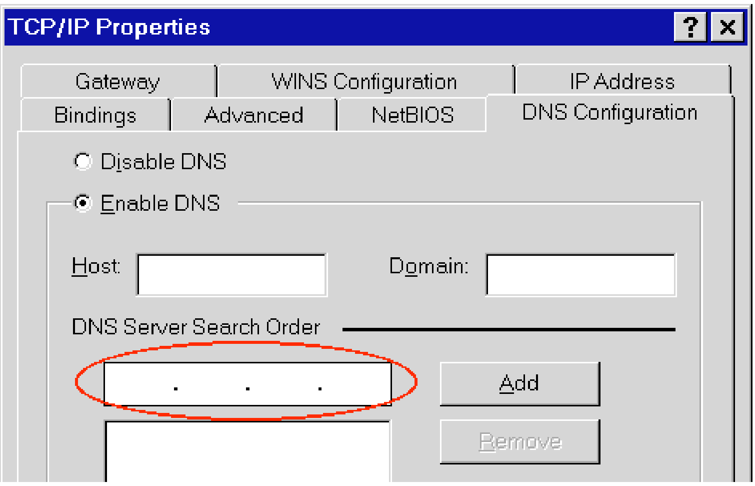


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192 . 168 . 0 . 1

Figure 8: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, and then click *Add*.



○ Disable DNS
● Enable DNS

Figure 9: DNS Tab (Win 95/98)

Note!

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to ***Chapter 8 - Routing*** *for details.*

Internet Access Configuration

If you are using the UGate-3200P for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select *"I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)"* and click "Next".
4. Select *"I connect through a local area network (LAN)"* and click "Next".
5. Ensure all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
6. Check the "No" option when prompted “Do you want to set up an Internet mail account now?”
7. Click "Finish" to close the Internet Connection Wizard.
8. Then simply use your Browser, FTP client, or other Internet client to connect to the desired Internet site.

Accessing AOL

To access AOL (America On Line) through the UGate-3200P, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "UGate-3200P".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "UGate-3200P" location.

Printing Setup

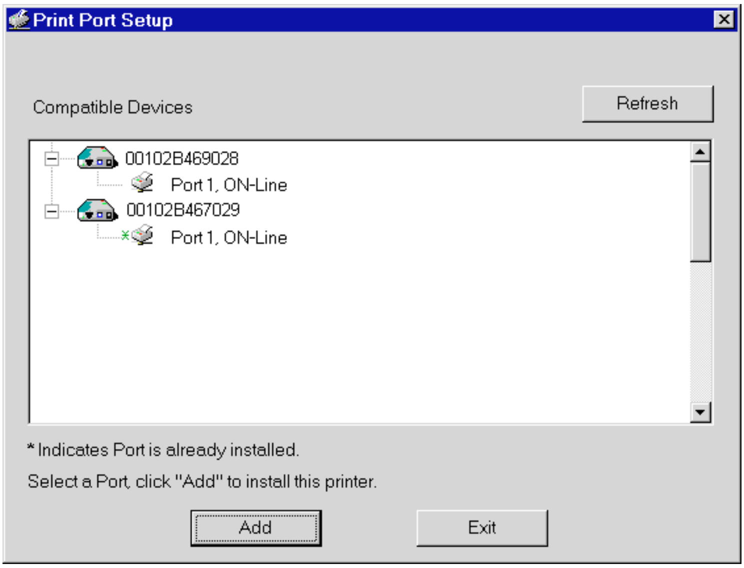
The UGate-3200P provides printing support for 2 methods of printing from Windows:

- **Print Port Driver.** After installing the Print Port Driver, Windows users can print directly to the UGate-3200P. Print jobs are spooled (queued) on each PC.
  The supplied Print Port Driver supports Windows 95/98, Windows NT4.0, Windows Me, and Windows 2000.
- **LPD Printing.** If using Windows NT 4.0 Server, LPD printing can be used. No software needs to be installed on either the Windows NT Server or each client PC. Print jobs will be spooled (queued) on the Windows NT Server, and can be managed using the standard Windows NT Server tools.

Printer Port Driver Setup

The following procedure is for Windows 95/98, Windows NT4.0, Windows Me, and Windows 2000.

1. Insert the supplied CD-ROM into your drive. If the setup program does not start automatically, run SETUP in the root folder.
2. Select the correct model, then the ***Printer Port Driver*** installation option.
3. Follow the prompts to complete the installation.
4. The *Print Port Setup* will then run, and the following screen will be displayed.



00102B469028
Port 1, ON-Line
00102B467029
Port 1, ON-Line

* Indicates Port is already installed.
Select a Port, click "Add" to install this printer.

Figure 10: Add Port (Peer-to-peer Print Driver)

5. Select the desired device and port, and then click the "Add" button.
6. A pop-up message will inform you if the port has been created successfully, and then the Windows *Add Printer* wizard will start.

  - Select the correct Printer Manufacturer and Model, or use the "Have Disk" option if appropriate.
  - We recommend changing the Printer name to indicate which device is on.
    (e.g. HP2100 on SCA43600_P1)

7. Installation is now complete. You can now print using this printer.
   - To install additional Printers, repeat steps 6 and 7.
   - Use the ***Start*** menu to run this program in future. The default installation is *Start - Programs - Print Server Utility - Print Server Setup*.

Management

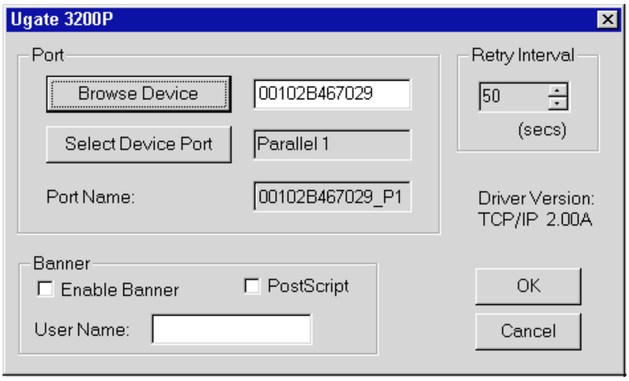
- Print jobs can be managed like any Windows printer. Open the *Printers* folder (*Start - Settings - Printers*) and double-click any printer to see the current print jobs.
- If the printer attached to the PrintMate is changed, just run this program again, and select the correct printer.
- To delete a port created by this setup program, use the Windows *Delete Port* facility:
  - Right-click any printer in the *Printers* folder, and select *Properties*.
  - Locate the *Delete Port* button. This button is on the *Details* or *Ports* tab, depending on your version or Windows.
- If the PrintMate's IP Address is changed, and you can no longer print, delete the port (see procedure above) and re-install it.

Port Options

The options for the *Print Port Driver* are accessed via the Windows *Port Settings* button.

Use *Start - Settings - Printers* to open the Printers folder, then right-click the Printer, and select *Properties*. The *Port Settings* button is on the *Details* or *Port* tab, depending on your version of Windows.

An example screen is shown below:



Browse Device: 00102B467029
Select Device Port: Parallel 1
Port Name: 00102B467029_P1
Retry Interval: 50 (secs)
Driver Version: TCP/IP 2.00A
☐ Enable Banner
☐ PostScript
User Name:

Figure 11: Port Settings (Peer-to-peer Driver)

Items shown on this screen are as follows:

Port	If desired, click *Browse* to select a different device. Note that the *Select Device Port* will not work on this model. The *Port Name* is shown in the Printer's *Properties*.
Banner	Check this option to print a banner page before each print job. • If using a PostScript Printer, check the *PostScript* box. • The *User Name* will be printed on the banner page.
Retry Interval	Sets how often Windows will poll the PrintMate to establish a connection when the printer is busy. Increase this value if you get too many warning messages.

LPD Printing

LPD printing can be used with Windows NT 4.0 Server. No software needs to be installed.

Windows NT 4.0 Server Configuration

To use LPD printing, **Microsoft TCP/IP Printing** must be installed and enabled. This can be checked using *Start-Settings-Control Panel-Network - Services*.

To install LPD printing using the UGate-3200P, follow this procedure:

1. Go to *Start-Settings-Printer* and invoke the *Add Printer* wizard.
2. When prompted with This printer will be managed by, select **My Computer** and click Next.
3. Select **Add Port…**, then select **LPR Port** and click **New Port**.
4. In the *Name of Address of server providing LPD* : Dialog box, enter the IP address of the UGate-3200P.
5. In the *Name of printer or print queue on that server* dialog box, enter L1
6. Click OK. When returned to the Printer Ports window, simply select *Close* and then install your printer driver as usual.
7. When prompted whether or not the printer will be shared, select the **Sharing** radio button.
8. In the *Shared* dialog box, enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
9. Click OK to save and exit.

PC Configuration for LPD Printing

The following procedure is for Windows 95/98, Windows NT4.0, Windows Me, and Windows 2000.

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Network Printer*.
3. When prompted for *Network Path or Queue Name*, click the *Browse* button, and locate the Server and Printer that your Network Administrator advised you to use.
4. Click OK, then *Next*.
5. Select the correct printer Manufacturer and Model, as advised by your Network Administrator, and click *Next*.
6. Follow the prompts to complete the Wizard.
7. The new printer will be listed with any other installed printers, any may be selected when printing from any Windows application.

Chapter5

Basic Setup

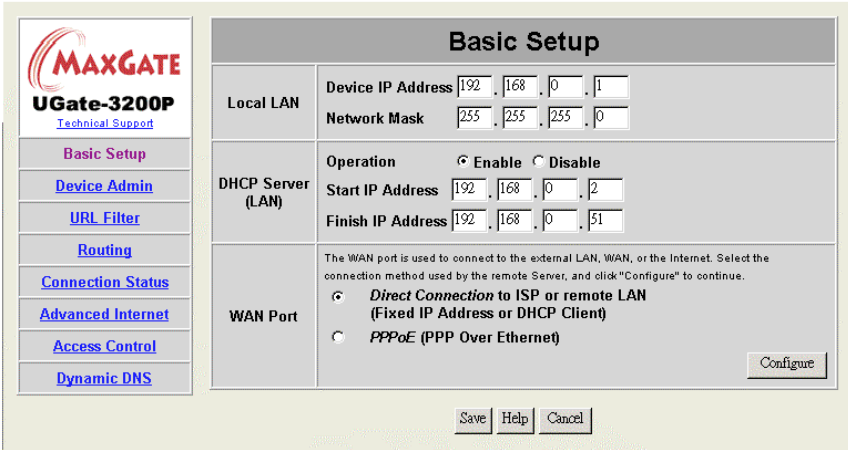
This Chapter describes the Basic Setup required to make your UGate-3200P operational.

Connecting to the UGate-3200P

Use your Web browser to connect to the UGate-3200P, as described in ***Chapter 3 - Configuration***.

Basic Setup Screen

The Basic Setup screen, like the example below, will be displayed when you first connect.



Basic Setup

Local LAN

Device IP Address 192 . 168 . 0 . 1

Network Mask 255 . 255 . 255 . 0

DHCP Server (LAN)

Operation ● Enable ○ Disable

Start IP Address 192 . 168 . 0 . 2

Finish IP Address 192 . 168 . 0 . 51

WAN Port

The WAN port is used to connect to the external LAN, WAN, or the Internet. Select the connection method used by the remote Server, and click "Configure" to continue.

● *Direct Connection* to ISP or remote LAN (Fixed IP Address or DHCP Client)

○ *PPPoE* (PPP Over Ethernet)

Figure 12: Basic Setup Screen

This screen has 3 sections:

- Local LAN
- DHCP Server (LAN)
- WAN Port

Local LAN

For most users, the default values for these fields should be satisfactory, and no changes will be required.

Data – Local LAN

IP Address	IP address for the UGate-3200P. Use the default value of 192.168.0.1 unless it is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address selected from the range used on your LAN.
Network Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the same value as the PCs connected to the UGate-3200P.

DHCP Server

A DHCP (Dynamic Host Configuration Protocol) **server** allocates a valid IP address to a DHCP **client** (PC or device) upon request.

- The client request is made when the client device boots.
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- By default, Windows 9x systems act as a DHCP **clients**.
- The UGate-3200P can act as a **DHCP server**.

Data – DHCP Server

Operation	If Enabled (default), the UGate-3200P acts as a DHCP Server. **If using another DHCP Server, this setting must be DISABLED, and the existing DHCP server must be re-configured to provide the UGate-3200P's IP Address as the *Default Gateway*.**
Start IP Address **Finish IP Address**	The *IP Start Address* and *IP Finish Address* fields set the values used by the DHCP server. This range also determines the number of DHCP clients supported. (Maximum 253.)

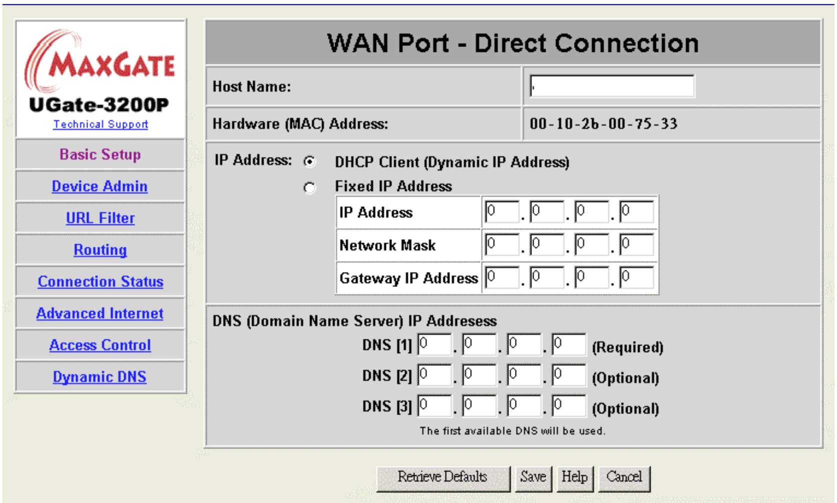
WAN Port

To configure the WAN port:

1. Save the data on the *Basic Setup* Screen.
2. Select the appropriate connection type (*Direct Connection* or *PPPoE*). If your connection documentation does not refer to *PPPoE*, select ***Direct Connection***.)
3. Click the “Configure” button.

4. You will then see either the *WAN Port - Direct Connection* screen or the *WAN Port - PPPoE* screen.

WAN Port - Direct Connection



WAN Port - Direct Connection

Host Name:	
Hardware (MAC) Address:	00-10-2b-00-75-33

IP Address: ● DHCP Client (Dynamic IP Address)
○ Fixed IP Address

IP Address	0 . 0 . 0 . 0
Network Mask	0 . 0 . 0 . 0
Gateway IP Address	0 . 0 . 0 . 0

DNS (Domain Name Server) IP Addresess

DNS [1] 0 . 0 . 0 . 0 (Required)
DNS [2] 0 . 0 . 0 . 0 (Optional)
DNS [3] 0 . 0 . 0 . 0 (Optional)

The first available DNS will be used.

Figure 13: WAN - Direct Connection

Data - WAN (Direct Connection)

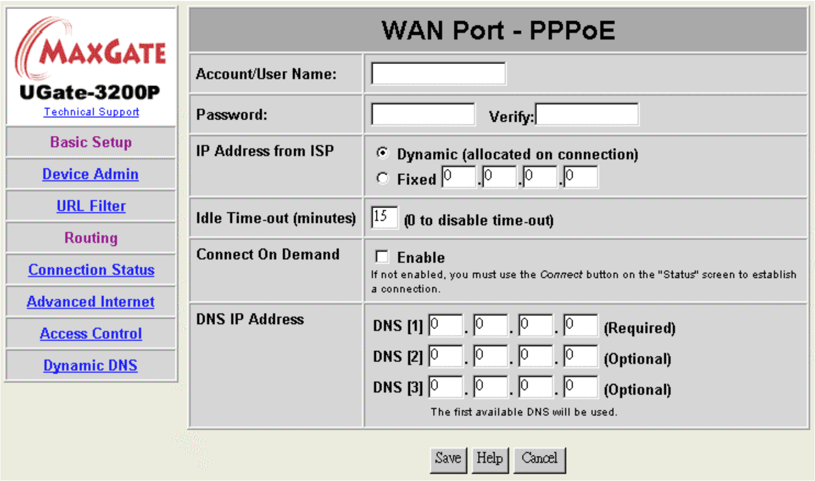
Device Name	Used for identification. Normally, there is no need to change the default name, but if your ISP requests that you use a particular “Hostname”, enter it here. This name will be provided to, and recorded by, the remote DHCP Server.
Hardware (MAC) Address	Also called *Network Adapter Address* or *Physical Address*. Provide this value to your ISP if requested. If you did not provide this value when first connected, there is no need to provide it now.
IP Address	
Dynamic IP Address	Leave this enabled if you want your ISP to allocate an IP Address to the UGate-3200P upon connection.
Fixed IP Address	Select this if using a fixed IP Address. If this option is selected, the following data must be entered. • **IP Address**. If connecting to an ISP, this is the address allocated by the ISP. (If connecting to another LAN, this must be a valid address on the remote LAN.) • **Network Mask** This must be compatible with the IP Address above • **Gateway IP Address** The address of the router or gateway supplied by your ISP. (If connecting to another LAN, this must be the

	gateway associated with the IP address above.)
DNS (Domain Name Server)	
DNS (Domain Name Server) IP Addresses	If your ISP uses a "Dynamic IP Address", then the DNS is also provided dynamically. Any DNS values entered here will be used instead of the dynamically obtained DNS addresses. If using a "Fixed IP Address", your ISP should recommend a DNS. If they don't, you can copy the public DNS entry from DNS (3) to DNS (1). Multiple DNS entries should be entered in the order you want them accessed. (The first available DNS will be used.)
Buttons	
Retrieve Defaults	Display the default values for this screen. The data is not saved unless you click the "Save" button.
Save	Save any data you have entered on this screen.
Cancel	Cancel any data entered since the last "Save" operation.

Notes:

- If using *Dynamic IP Address*, the IP Address, Network Mask, and Gateway fields may display the values obtained dynamically.
- The *Retrieve Defaults* button will recover the default *Device Name* and clear the other items. No changes are made to the configuration until you click the *Save* button.

WAN Port - PPPoE



WAN Port - PPPoE

Account/User Name:	
Password:	Verify:
IP Address from ISP	● Dynamic (allocated on connection) ○ Fixed 0 . 0 . 0 . 0
Idle Time-out (minutes)	15 (0 to disable time-out)
Connect On Demand	☐ Enable If not enabled, you must use the *Connect* button on the "Status" screen to establish a connection.
DNS IP Address	DNS [1] 0 . 0 . 0 . 0 (Required) DNS [2] 0 . 0 . 0 . 0 (Optional) DNS [3] 0 . 0 . 0 . 0 (Optional) The first available DNS will be used.

Figure 14: WAN Port - PPPoE

Data – WAN (PPPoE)

Account/ User Name	The name of the Internet account provided by your ISP.
Password & Verify	Enter the password for the above account. Re-enter the password in the *Verify* field, to ensure it is correct.
IP Address provided by ISP	Normally, this is *Dynamic*; use this setting if your ISP's data does not mention an IP Address. If your ISP did provide an IP Address, select *Fixed* and enter the value they provided.
Connect on Demand	Normally, this should be Enabled. If disabled, only the *Connect* button (***Status*** screen) can establish a connection.
Idle Time-out	If a connection is inactive for longer than this time period, it will be terminated. Zero (0) means never to terminate.
DNS (Domain Name Server)	
DNS (Domain Name Server) IP Addresses	If your ISP uses a “Dynamic IP Address”, then the DNS is also provided dynamically. Any DNS values entered here will be used instead of the dynamically obtained DNS addresses. If using a “Fixed IP Address”, your ISP should recommend a DNS. If they don't, you can copy the public DNS entry from DNS (3) to DNS (1). Multiple DNS entries should be entered in the order you want them accessed. (The first available DNS will be used.)
Buttons	
Save	Save any data you have entered on this screen.
Cancel	Cancel any data entered since the last "Save" operation.

Chapter 6

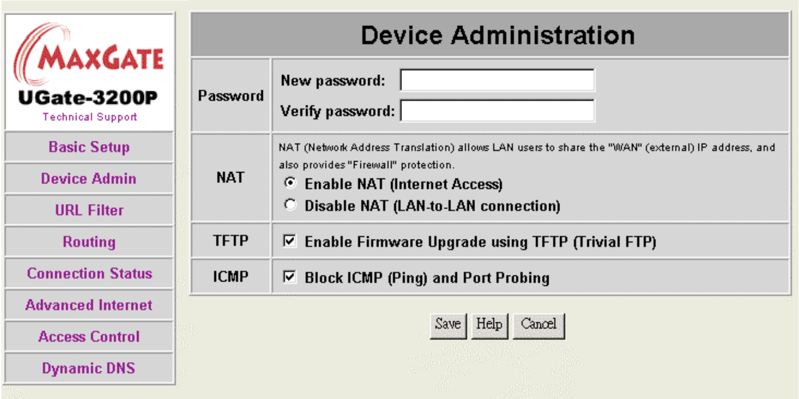
6

Device Administration

This Chapter details the settings available on the UGate-3200P's "Device Admin" screen.

Overview

The *Device Administration* screen is accessed via the *Device Admin* menu option. An example screen is shown below.



Device Administration

Password	New password: Verify password:
NAT	NAT (Network Address Translation) allows LAN users to share the "WAN" (external) IP address, and also provides "Firewall" protection. ● Enable NAT (Internet Access) ○ Disable NAT (LAN-to-LAN connection)
TFTP	☑ Enable Firmware Upgrade using TFTP (Trivial FTP)
ICMP	☑ Block ICMP (Ping) and Port Probing

Figure 15: Device Administration Screen

Password

Once a password is entered, it is required in order to change the device configuration. Passwords are case sensitive and can be up to 8 alphanumeric characters (no spaces or punctuation).

To create or change the password, enter the required password in both the *New Password* and *Verify Password* input fields.

Note!

When prompted for the password, leave the "User Name" blank.

NAT (Network Address Translation)

NAT allows PCs on your LAN to share a single external (Internet) IP Address. This IP Address is supplied by your ISP. Use the following to determine whether or nor you need NAT.

- For Internet access, NAT **must be left On** unless all PCs on your LAN have valid external IP Addresses.
- If this device is not being used to provide shared Internet access, NAT is not normally required. With NAT disabled, the UGate-3200P will act as a static router.
- If NAT is disabled, the Firewall protection provided by the UGate-3200P is lost, and the *Advanced Internet* features (Virtual Servers, Special Applications, and DMZ) are no longer available.

TFTP

TFTP (Trivial FTP) can be used to upgrade the firmware in the UGate-3200P. However, this is not normally required; there is a Windows utility available for this purpose.

ICMP

A device, often a router, to report and acquire a wide range of communications-related information, such as echo, echo reply, timestamp and etc., uses Internet Control Message Protocol (ICMP).However, ICMP can also have a negative effect on your network’s security. For instance, ICMP can be employed in scanning networks to locate where you are.

By default “Block ICMP and Probing” function is enabled on the UGate-3200P. That means it is impossible to use any ICMP command from remote sites to reach the UGate-3200P, such as ping, tracer, etc. Moreover, all of the tested ports were shown to have stealth (filtered) status from port scanning software and as a result your computer doesn't exist to scanners on the Internet. This means either your computer is turned off or disconnected from the Net (which seems unlikely since you must be using it right now!) or an effective stealth firewall is blocking all unauthorized external contact with your computer.

Chapter 7

URL Filter

This Chapter explains how to use the UGate-3200P's "URL Filter" feature.

Overview

The URL Filter provides a means to block access to undesirable Web sites.

If a site address is entered on the URL Filter screen, access to that site is blocked when the URL Filter is enabled.

- The blocking action applies to all PCs accessing the Internet via the UGate-3200P.
- Only the HTTP protocol, as used by Web Browsers, is blocked. Other protocols, such as FTP and SMTP (E-Mail), are not affected.
- Either compete or partial Web site addresses may be entered.

The URL Filter feature in the UGate-3200 works by matching text strings entered in the URL Filter against the requested URL. For example, by inputting the word “bad” in the URL Filter, any URL containing the letters “bad” in it will be blocked.

To use the feature properly, you should try inputting as much of the text for the given URL as possible. For example, instead of simply using the word “bad,” you would use the full web site name, which might be “www.badsite.com.” You may also make the text string even longer to be more specific. If you did not want to block an entire web site, you could include more of the URL. For example, “www.badsite.com/badsection/”

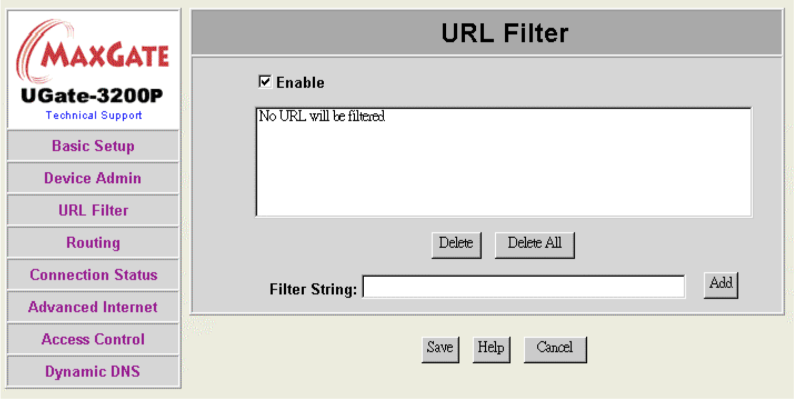
So, please careful when using the URL Filter, as a general word might block access to a site that is desired.

Using the URL Filter

1. Enable the URL Filter on the ***URL Filter*** screen.
2. Enter the full or partial URLs of the sites you wish to block.
3. Save the data, and use the UGate-3200P normally.
4. Later, check the Outgoing Access Log to see which sites have been blocked.
    - The button to view the Access Log is on the ***Connection Status*** screen.
    - This information can be used to "fine-tune" your URL Filter list.

URL Filter Screen

This screen is reached via the ***URL Filter*** menu option. An example screen is shown below.



☑ Enable

No URL will be filtered

Filter String:

Figure 16: URL Filter Screen

Enable	This must be checked for the URL Filter to be active.
URL Filter list	This window lists all the Filter strings you have entered.

Filter String	Enter the text string that you wish to block. Either complete or partial addresses may be used. For example, each of the following is a valid entry.
	www.unwanted.com/unwanted/unwanted.html
	`www.unwanted.com`
	`unwanted`

Buttons	
Delete	This button will delete the selected entry in the main URL Filter list. To select an entry, single click on it first. To select multiple entries, hold down the CTRL key (Windows) or SHIFT key (Mac) while selecting.
Delete All	This button will delete all entries in the main URL Filter list.
Add	This button adds the current text in the Filter String field to the main URL Filter list.
Save	This button is used to save the setting for the Enable button.
Help	View the help file for this screen.
Cancel	This button will cancel any information not saved previously using the "Save" or "Add" buttons.

Chapter 8
Routing

This Chapter explains the Routing features of the UGate-3200P.

Overview

While the UGate-3200P includes a standard (static) routing table, this feature can be completely ignored if you do not have a router in your LAN.

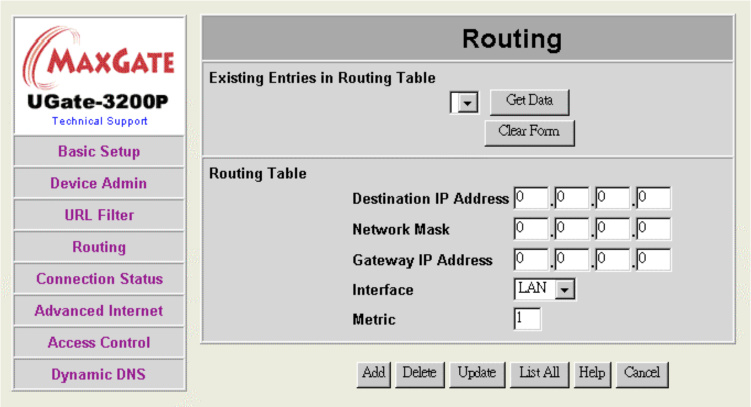
If you DO have a router, it is necessary to configure BOTH the Router and the Routing table in the UGate-3200P correctly, as described in the following sections.

Note!

See page 31 for an example of configuring both the UGate-3200P and the Router.

UGate-3200P Configuration

The routing table is accessed by the *Routing* link on the LAN screen. An example screen is shown below.



Destination IP Address: 0 . 0 . 0 . 0
Network Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0
Interface: LAN
Metric: 1

Figure 17: Routing Screen

Using this Screen

Any existing entries are listed.

- To view and edit the details of an existing entry, select it, and click "Get Data". After editing, click the "Update" button to save your changes.
- To add a new entry, click "Clear Form", enter your data, and then click the "Add" button.
- To delete an entry, select it, then click the "Delete" button.

Routing Table Data

An entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached. The data in the Routing Table is as follows.

Destination IP Address	The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of this *Destination IP Address*. The 4th (last) field can be left at 0.
Network Mask	The Network Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0
Gateway IP Address	The IP Address of the Router on the LAN segment to which this device is attached. (NOT the router on the remote LAN segment.)
Interface	Select the appropriate interface - LAN or WAN) from the drop-down list.
Metric	The number of routers that must be traversed to reach the remote LAN segment. The default value is 1.

Router Configuration

It is essential that all IP packets for devices not on the local LAN be passed to the UGate-3200P, so that they can be forwarded to the WAN or Internet. To achieve this, the local LAN must be configured to use the UGate-3200P as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the UGate-3200P. This router requires that the *Default Route* is the UGate-3200P itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the UGate-3200P.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the UGate-3200P's *Local Router* as the *Default Route*. The entries will be the same as the UGate-3200P's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the 's local Router, the *Gateway IP Address* is the address of the UGate-3200P's local router.
- For routers that must forward packets to another router before reaching the UGate-3200P's local router, the *Gateway IP Address* is the address of the intermediate router.

Routing Example

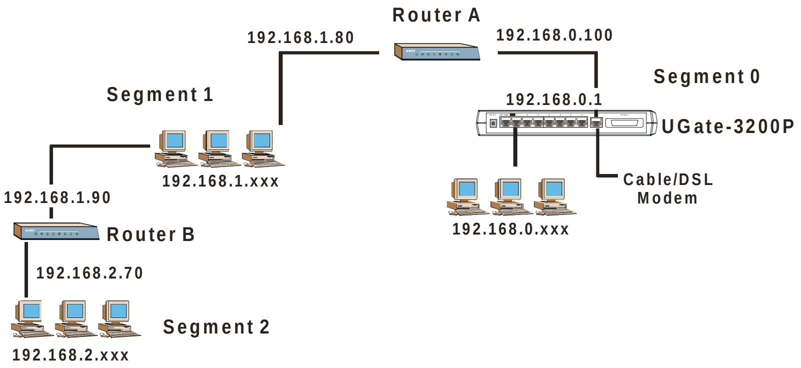


Figure 18: Routing Example

For the LAN shown above, with 2 routers and 3 LAN segments, the required entries would be as follows.

For the UGate-3200P's Routing Table

The UGate-3200P requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (UGate-3200P's local Router)
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.0.100

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (UGate-3200P's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (UGate-3200P's local router)

Chapter 9

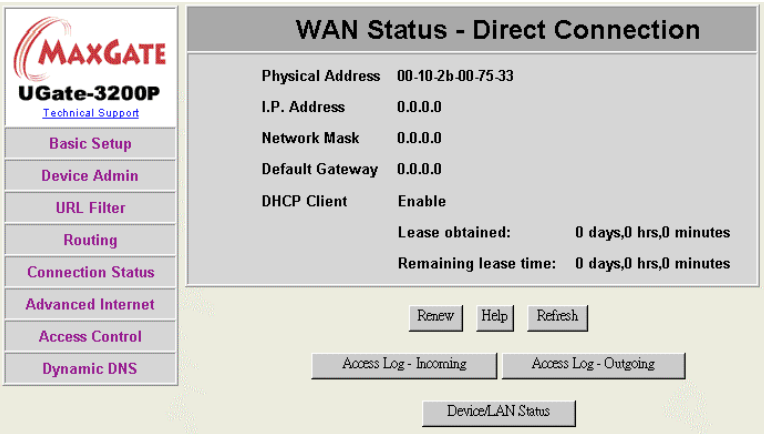
Status Screens

This Chapter details the various status screens provided by the 3200P.

WAN Status

Clicking ***Connection Status*** on the menu bar will take you to the ***WAN Status*** screen. The screen shown will depend on whether you are using a **Direct Connection** or **PPPoE**.

WAN Status – Direct Connection



WAN Status - Direct Connection

Physical Address 00-10-2b-00-75-33
I.P. Address 0.0.0.0
Network Mask 0.0.0.0
Default Gateway 0.0.0.0
DHCP Client Enable
Lease obtained: 0 days,0 hrs,0 minutes
Remaining lease time: 0 days,0 hrs,0 minutes

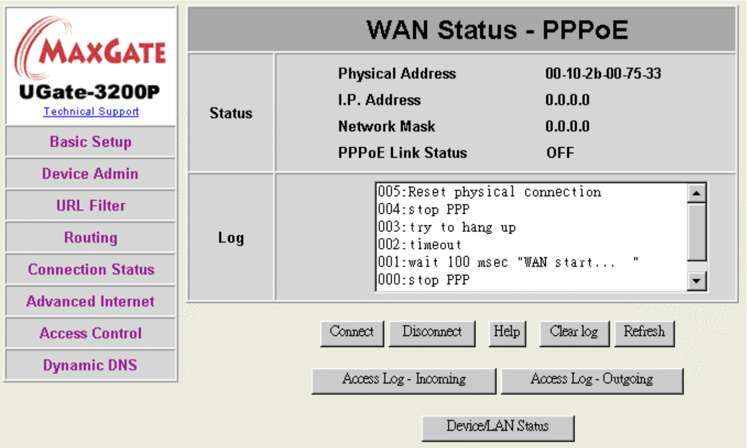
Figure 19: WAN Status – Direct Connection

Status Screen - Direct Connection

Physical Address	The "Hardware" address of this device, as seen by other devices on the WAN port.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask for the above IP Address.
Default Gateway	IP address of the Router/Gateway on the WAN port.
DHCP Client	Displays "Enabled" or "Disabled", indicating whether this device is acting as a DHCP client on the WAN port.

Buttons	
Renew	Use this button if the connection seems to have been lost, and no data is being transferred. (This button has no effect unless acting as a DHCP Client.)
Refresh	Update the data on screen.
Access Log – Incoming	List the access requests made from the WAN (Internet) interface to devices on your LAN. See page 36 for further details.
Access Log – Outgoing-	List the access requests made by PCs on your LAN to Internet sites. See page 36 for further details.
Device/LAN Status	Jump to the Device/LAN status screen. See page 37 for details.

WAN Status – PPPoE



Physical Address 00-10-2b-00-75-33
I.P. Address 0.0.0.0
Network Mask 0.0.0.0
PPPoE Link Status OFF

```
005:Reset physical connection
004:stop PPP
003:try to hang up
002:timeout
001:wait 100 msec "WAN start...   "
000:stop PPP
```

Figure 20: WAN Status – PPPoE

Status Screen - PPPoE

Status	
Physical Address	The hardware address of this device.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.

PPPoE Link Status	This indicates whether or not the connection is currently established. If the connection does not exist, the ***Connect*** button can be used to establish a connection. If the connection currently exists, the ***Disconnect*** button can be used to break the connection.
Log	
	The Connection Log shows status messages relating to the existing connection. The most common messages are listed in the table below.
Buttons	
Connect	If not connected, establish a connection to your ISP
Disconnect	- If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Contact this device and update the Log data.
Access Log – Incoming	List the access requests made from the WAN (Internet) interface to devices on your LAN. See page 36 for further details.
Access Log – Outgoing-	List the access requests made by PCs on your LAN to Internet sites. See page 36 for further details.
Device/LAN Status	Jump to the Device/LAN status screen. See page 37 for details.

Connection Log Mesages

Message	**Description**
Connect on Demand	Connection attempt has been triggered by the "Connect on Demand" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.

Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

Access Logs

The Access Log buttons allow you to view incoming and outgoing requests.

Access Log – Incoming

This displays the access requests made from the WAN (Internet) interface to devices on your LAN.

Access Log- Incoming	
IP Address	Displays the IP address of the remote computer accessing your LAN
Port No:	Displays the port number being used by the remote computer for this access request.

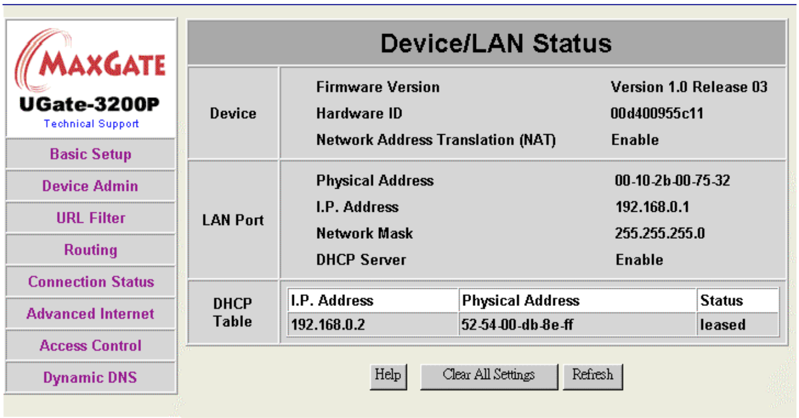
Access Log – Outgoing

This displays the access requests made by PCs on your LAN.

Access Log- Outgoing	
IP Address	Displays the IP address of the local computer which made this request.
URL	Displays the URL requested by the computer above.
Blocked	Indicates whether or not the URL request was blocked by the URL Filter. For full details of the URL Filter, refer to ***Chapter 7 - URL Filter***.

Device/LAN Status

The ***LAN Status*** link on the menu will result in a screen like the example below.



Device/LAN Status

Device	Firmware Version	Version 1.0 Release 03
	Hardware ID	00d400955c11
	Network Address Translation (NAT)	Enable
LAN Port	Physical Address	00-10-2b-00-75-32
	I.P. Address	192.168.0.1
	Network Mask	255.255.255.0
	DHCP Server	Enable

DHCP Table

I.P. Address	Physical Address	Status
192.168.0.2	52-54-00-db-8e-ff	leased

Figure 21: Status Screen

Data – Device/LAN Status

Device	
Firmware Version	Version of the firmware (embedded software, including this program) which is currently installed.
Hardware ID	The hardware ID of this device, used by the manufacturer.
Network Address Translation	This will display "Enabled" or "Disabled", indicating whether or not NAT is in use. This setting is on the ***Device Admin*** screen.
LAN Port	
Physical Address	The "Hardware" address of this device, as seen by other devices on the local LAN.
IP Address	The IP Address of this device, as seen by other devices on the local LAN.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
DHCP Table	
IP Address	The IP Address which has been allocated by the DHCP server to the other device.
Physical Address	The Physical Address (Hardware Address) of the device that has been allocated an IP Address.

Status	Possible Status values are "Leased" (the IP Address is allocated to the device shown) or "Reserved" (the IP Address is not available).

Note:

The DHCP table will be empty unless the DHCP Server function is being used. If not empty, this table lists the devices on the LAN that have been allocated IP Addresses by the DHCP server function.

Chapter 10

Advanced Internet

This Chapter explains how to use the UGate-3200P's "Advanced Internet" features.

Overview

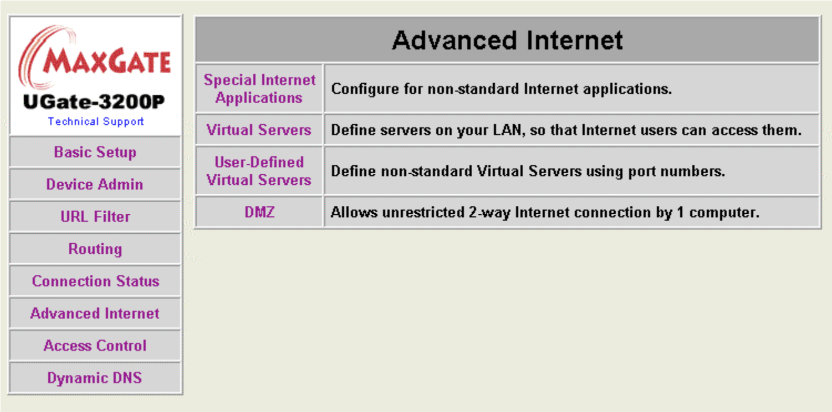
For situations where the UGate-3200P is being used to provide shared Internet access, the following advanced features are provided.

- Special Applications
- Virtual Servers
- DMZ

This chapter contains details of the configuration and use of each of these features.

Advanced Internet Screen

This screen provides access to the advanced Internet features. A sample screen is shown below.



Advanced Internet

Special Internet Applications	Configure for non-standard Internet applications.
Virtual Servers	Define servers on your LAN, so that Internet users can access them.
User-Defined Virtual Servers	Define non-standard Virtual Servers using port numbers.
DMZ	Allows unrestricted 2-way Internet connection by 1 computer.

Figure 22: Advanced Internet Screen

Use the sub-menu to navigate to the desired screen.

Special Applications

This feature is only required if you wish to use Internet applications which require 2-way communication, multiple connections, or combined TCP/UDP connections.

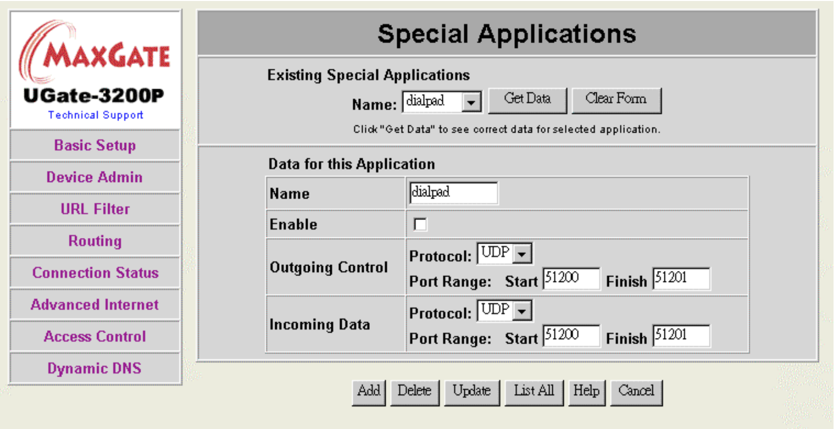
Examples of such applications are Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers.

Generally, you will become aware of the need for this feature when an Internet application is unable to function correctly.

> Note!
>
> *At any time, only one (1) PC can use each Special Application.*

Special Applications Screen

This screen can be reached by selecting *Advanced Internet - Special Applications*. An example screen is shown below.



Special Applications

Existing Special Applications

Name: dialpad

Click "Get Data" to see correct data for selected application.

Data for this Application

Name	dialpad
Enable	☐
Outgoing Control	Protocol: UDP Port Range: Start 51200 Finish 51201
Incoming Data	Protocol: UDP Port Range: Start 51200 Finish 51201

Figure 23: Special Applications Screen

Using a Special Application

- Existing entries only need to be enabled. (As shipped, some Special Applications have been defined not enabled.)
- For new entries, configure the *Special Applications* screen as required.

> Note!
>
> *Configuration data must be obtained from the Service/Application provider.*
> *If an application still cannot function correctly, try using the "DMZ" feature.*

- **To Enable a defined Application**
  Select it from the drop-down list
  Click "Get Data"
  Check the *Enable* checkbox
  Click "Update"

- **To Disable a defined Application**
  As above, but uncheck the *Enable* checkbox.
- **To Delete a defined Application**
  Select it from the drop-down list,
  Click "Delete"
- **To Modify (Edit) a defined Application**
  Select it from the drop-down list,
  Click "Get Data"
  Make any desired changes
  Click "Update"
- **To Create a new Application**
  Click "Clear Form"
  Enter the required data, as described below
  Click "Add"
- **To List all Applications**
  Click "List All"

Configuration Data (from Service Provider)

This data must be obtained from the service provider.

Name	Enter a descriptive name to identify this application entry.
Enable	Use this to Enable or Disable support for this application, as required.
Outgoing Control	
Protocol	The protocol (TCP or UDP) used when you connect to the special application service.
Port Range: Start	The beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, for data you send.
Incoming Data	
Protocol	The protocol (TCP or UDP) used when the application or service sends data to you.
Port Range: Start	The start of the range of port numbers used by the application server when data is sent to you. If using only one port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, when data is sent to you.

Virtual Servers

This feature allows you to make a server on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

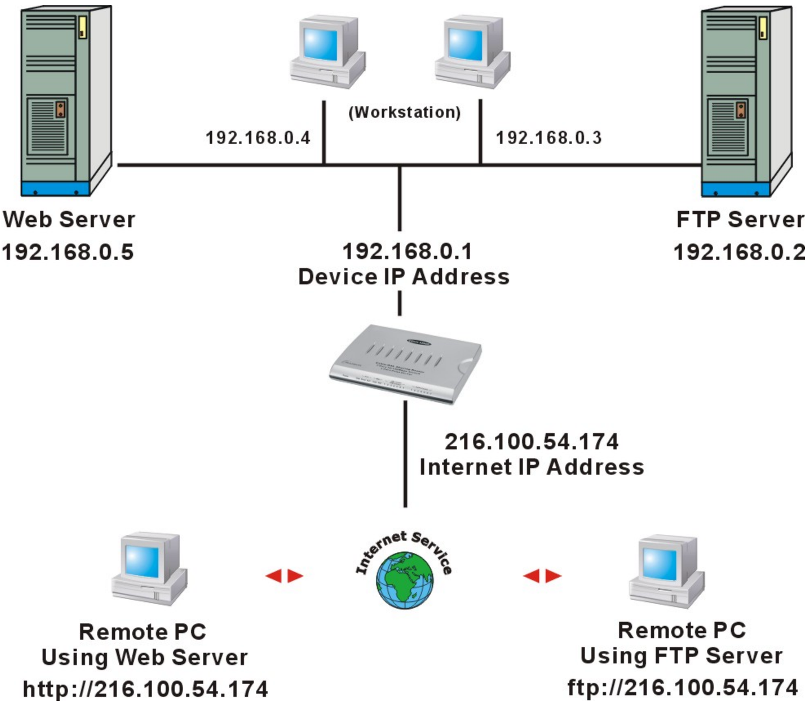


Figure 24: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address.

This IP Address is allocated by your ISP. It is shown as the *IP Address* on the *Connection Status* screen.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. If it is dynamic (allocated on connection), the Dynamic DNS feature is a great benefit. See Chapter 12 for details of the Dynamic DNS feature.

Types of Virtual Servers

The UGate-3200P supports two (2) types of Virtual Servers:

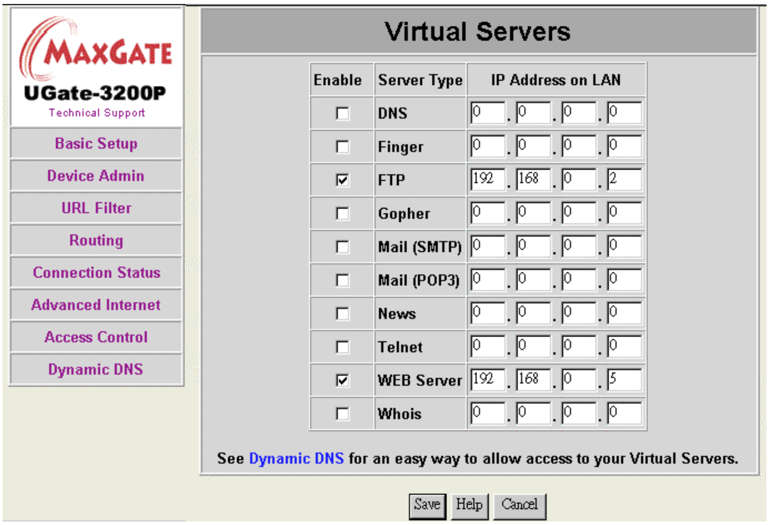
- **Pre-defined -** Standard server types. The only data required is the IP Address of the server on your LAN.
- **User-defined -** Non-standard servers. You must provide additional information about the server.

Note:

The TOTAL number of Virtual Servers that can be used at any time is 10.

Virtual Server Configuration

The *Virtual Server* screen is reached by the *Advanced Internet - Virtual Server* link. An example screen is shown below.



Virtual Servers

Enable	Server Type	IP Address on LAN
☐	DNS	0 . 0 . 0 . 0
☐	Finger	0 . 0 . 0 . 0
☑	FTP	192 . 168 . 0 . 2
☐	Gopher	0 . 0 . 0 . 0
☐	Mail (SMTP)	0 . 0 . 0 . 0
☐	Mail (POP3)	0 . 0 . 0 . 0
☐	News	0 . 0 . 0 . 0
☐	Telnet	0 . 0 . 0 . 0
☑	WEB Server	192 . 168 . 0 . 5
☐	Whois	0 . 0 . 0 . 0

See Dynamic DNS for an easy way to allow access to your Virtual Servers.

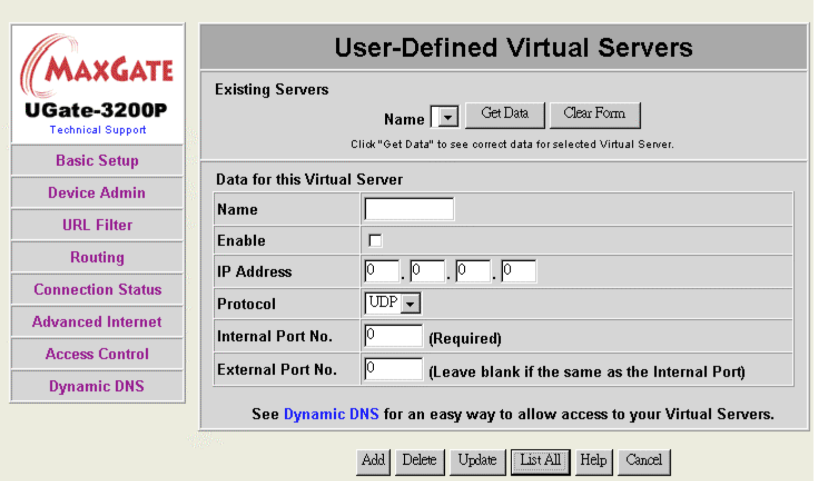
Figure 25: Virtual Server Screen.

Simply select the Server type or types you wish to use, enter the IP Address of the server on your LAN, and click "Save".

User Defined Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Server* screen, you can define it using this feature.

The screen for this function is reached by selecting *Advanced Internet - User Defined Virtual Servers*. An example screen is shown below.



Existing Servers

Name

Click "Get Data" to see correct data for selected Virtual Server.

Data for this Virtual Server

Name	
Enable	☐
IP Address	0 . 0 . 0 . 0
Protocol	UDP
Internal Port No.	0 (Required)
External Port No.	0 (Leave blank if the same as the Internal Port)

See Dynamic DNS for an easy way to allow access to your Virtual Servers.

Figure 26: User Defined Virtual Servers

This database operates in the same way as the other databases:

- **To Create a new Server**
  Click "Clear Form"
  Enter the required data (See next section)
  Click "Add"
- **To Modify (Edit) a defined Server**
  Select it from the drop-down list,
  Click "Get Data"
  Make any desired changes. Note that you can "Enable" and "Disable" a Server using this process.
  Click "Update"
- **To Delete a defined Server**
  Select it from the drop-down list,
  Click "Delete"
- **To List all Servers**
  Click "List All"

Configuration Data

Name	Enter a descriptive name to identify this Server entry.
Enable	Use this to Enable or Disable support for this Server, as required.
IP Address	The IP Address of the PC on your LAN which is running the Server software.

Protocol	Select the protocol (TCP or UDP) used by the Server.
Internal Port Number	Enter the port number used by the Server to connect to clients.
External Port Number	The port number used by clients when connecting to the Server. This is normally the same as the *Internal Port Number*. If it is different, this device will perform a "mapping" or "translation" function, allowing you to configure the server to use one port address, while clients use a different port address

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must enter the IP Address allocated by your ISP (shown as the *IP Address* on the *Connection Status* screen) as the destination.
e.g.

```
http://216.100.54.174
```

However, by using the ***Dynamic DNS*** feature, users can connect using your MaxGate-supplied domain name, rather than the IP Address. See Chapter 12 for details of the ***Dynamic DNS*** feature.

Using this Device as a Virtual Web Server

It is possible to configure the UGate-3200P itself as a Virtual Web Server. Once this is done, you can configure this device through the Internet.

For the remote PC, the destination IP Address is the IP Address as used by all Virtual Servers - the *IP Address* shown on the *Connection Status* screen.

Upon connecting to the UGate-3200P, you will be prompted for the device password. Leave the user name blank, and enter the password you have assigned to the Ugate-3200P.

Note!

Ensure that a password has been set!

To make the UGate-3200P a *Virtual Web Server*:

- Enable *Virtual Server* on the *Advanced Internet* screen
- Enable *Web Server* on the *Virtual Servers* screen.
- Enter the IP Address of the Ugate-3200P (the *Device IP Address* on the *Basic Setup* screen) as the IP Address of the Web Server.

DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the "DMZ" and other Internet users or Servers.

- Internet users will see the PC as having the *IP Address* allocated by your ISP (as shown on the *Connection Status* screen). This is the same IP Address used by the Virtual Servers.
- Any Internet user who knows this address can connect to the *DMZ*. (What happens after connection depends on what software both computers are using).
- If using the ***Dynamic DNS*** feature, Internet users can connect to the DMZ computer using your domain name, instead of your IP address. See Chapter 12 for details of the ***Dynamic DNS*** feature.

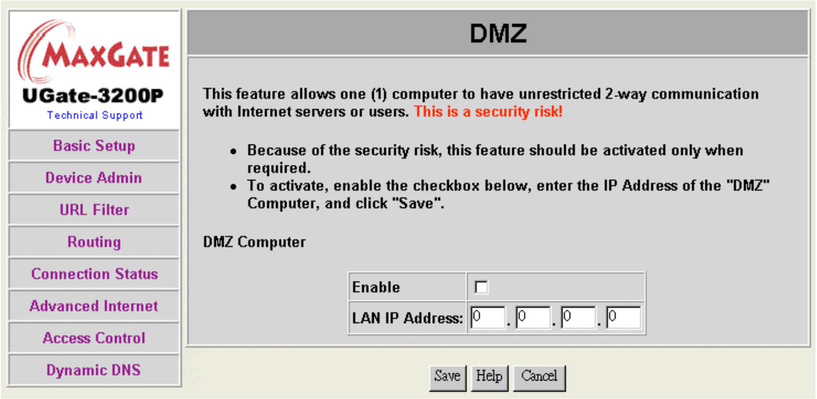
This allows for a connection to special-purpose servers, which require proprietary client software, or 2-way user connections such as Video-conferencing, which requires both users to run special software.

To allow unrestricted access, the Firewall in this device is disabled, creating a security risk.

- **You should use this feature only if the "Special Applications" feature is insufficient to allow an application to function correctly.**
- **This feature should be turned ON only when needed, and left OFF the rest of the time.**

Configuring the DMZ

Select *Advanced Internet* from the navigation bar, then *DMZ*. You will see a screen like the following:



DMZ

This feature allows one (1) computer to have unrestricted 2-way communication with Internet servers or users. This is a security risk!

- Because of the security risk, this feature should be activated only when required.
- To activate, enable the checkbox below, enter the IP Address of the "DMZ" Computer, and click "Save".

DMZ Computer

Enable	☐
LAN IP Address:	0 . 0 . 0 . 0

Figure 27: DMZ Screen

Data

The only data required is the *LAN IP Address*. Enter the IP Address of the PC on your LAN, which will become the "DMZ".

Chapter 11

Access Control

11

This Chapter explains how to configure and use the UGate-3200P's "Access Control" feature.

Overview

The Access Control feature allows administrators to restrict Internet Access by individual workstations. The process uses "Packet Filtering" to block or discard data packets. By default, no packets are blocked or discarded.

To use this feature:

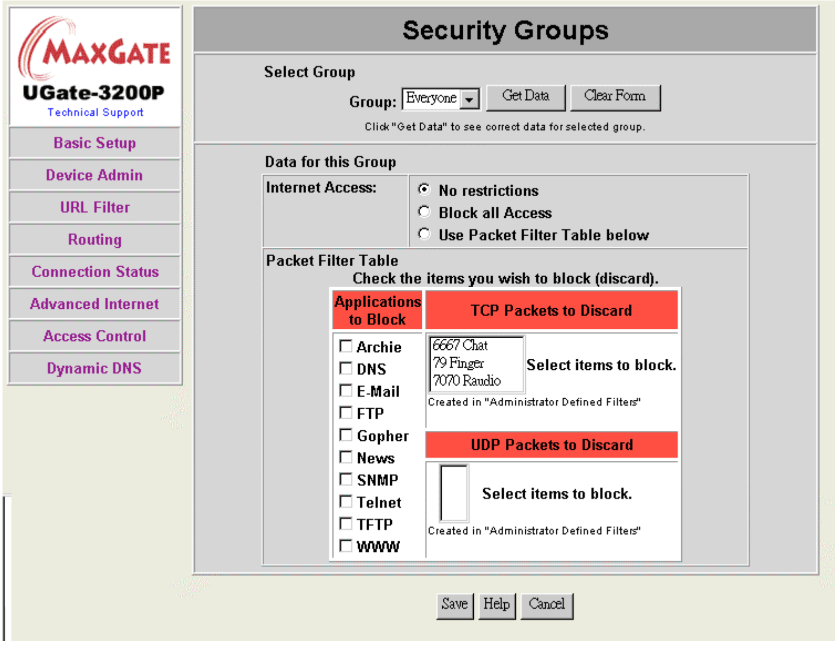
- Set the desired restrictions on the "Everyone" group. By default, all PCs are in the "Everyone" group unless explicitly moved to another group, using the *Workstation* screen.
- Set the desired restrictions on the other groups ("Group 1", "Group 2", etc) as needed.
- For each Workstation you wish to move from the "Everyone" group, enter their details on the *Workstation* screen, and assign them to the desired group

> *Note!* ☞ *You can limit Internet access for ALL PCs without entering ANY workstation data. Simply apply the desired restrictions to the "Everyone" group.*

It is also possible to define your own packet filters, and use these filters in addition to the pre-defined filters. Defining your own filters is optional.

Security Groups Screen

The *Security Groups* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



Security Groups

Select Group

Group: Everyone

Click "Get Data" to see correct data for selected group.

Data for this Group

Internet Access:
● No restrictions
○ Block all Access
○ Use Packet Filter Table below

Packet Filter Table

Check the items you wish to block (discard).

Applications to Block
☐ Archie
☐ DNS
☐ E-Mail
☐ FTP
☐ Gopher
☐ News
☐ SNMP
☐ Telnet
☐ TFTP
☐ WWW

TCP Packets to Discard
6667 Chat
79 Finger
7070 Raudio
Select items to block.
Created in "Administrator Defined Filters"

UDP Packets to Discard
Select items to block.
Created in "Administrator Defined Filters"

Figure 28: Security Groups Screen

Note that the Security groups are pre-named "Everyone", "Group 1", "Group 2", "Group 3", and "Group 4".

Operations

- **Initial Configuration:**
  Select the desired group from the drop-down box, then enter the required data as explained below. If necessary, click *Clear Form* to remove the existing information shown on screen.
  Click the *Save* button when finished.
- **To Change Access for a Group**:
  Select the group from the drop-down box, click *Get Data* to view their information, then change any fields you wish.
  Click *Save* when finished.
- **To Assign Workstations to a Security Group**
  All Workstations are automatically in the "Everyone" group. Use the *Workstations* screen to move them to another group if required.

Data

The following data is required.

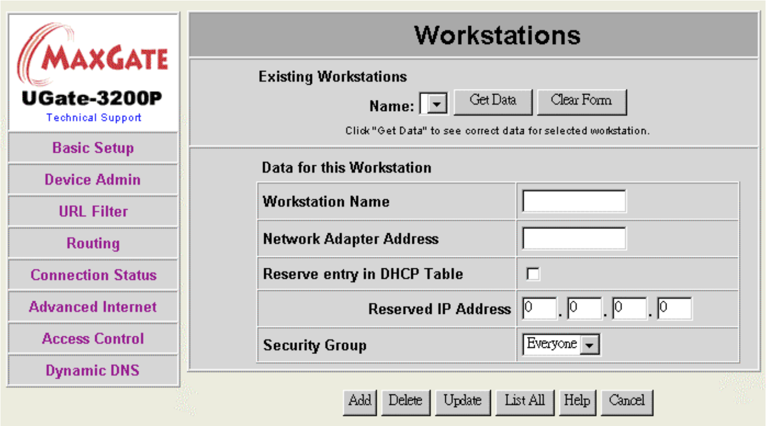
Internet Access for this Group	
No restrictions	No packets are blocked. Use this to create an "Unlimited Access" group, or to temporarily remove restrictions from a group.
Block all Access	Group members cannot access the Internet at all. Use this to create the most restrictive group.
Use Packet Filter Table below	Use this to define intermediate levels of access. Using the Packet Filter table gives you fine control over Internet access.
Packet Filter Table	
Applications to Block	Any items checked will be blocked. Users will not be able to use the application.
TCP Packets to Discard	This lists any TCP filters you have defined on the *Administrator Defined Filters* screen. If you have not defined any filters, this list is empty. Selected items can NOT be accessed by members of this group. Multiple items can be selected (or deselected) by holding down the CTRL key (Windows) or SHIFT key (Mac) while selecting items.
UDP Packets to Discard	This lists any UDP filters you have defined on the *Administrator Defined Filters* screen. If you have not defined any filters, this list is empty. Selected items can NOT be accessed by members of this group. Multiple items can be selected (or deselected) by holding down the CTRL key (Windows) or SHIFT key (Mac) while selecting items.

Note!

If you have not defined your own filters, but wish to do so, refer to "Administrator Defined Filters" on page 53.

Workstations

The *Workstations* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



Name:

Click "Get Data" to see correct data for selected workstation.

Workstation Name	
Network Adapter Address	
Reserve entry in DHCP Table	☐
Reserved IP Address	0 . 0 . 0 . 0
Security Group	Everyone

Figure 29: Workstations Screen

Note that the drop-down box lists all Workstations previously entered. If none have been entered, this box will be empty.

Operations

- **To Add a New Workstation**:
  Ignore the drop-down box, click the *Clear Form* button, and enter the Workstation details in the fields provided.
  Click *Add* when finished.
- **To Delete an Existing Workstation:**
  Select the Workstation from the drop-down box, click *Get Data* to view the information and confirm that this is the correct Workstation, then click the *Delete* button.
- **To Change an Existing Workstation's Details**:
  Select the Workstation from the drop-down box, click *Get Data* to view their information, then change any fields you wish.
  Click *Update* when finished.
- **To Generate a List of all Workstations:**
  Just click on the *List All* button.

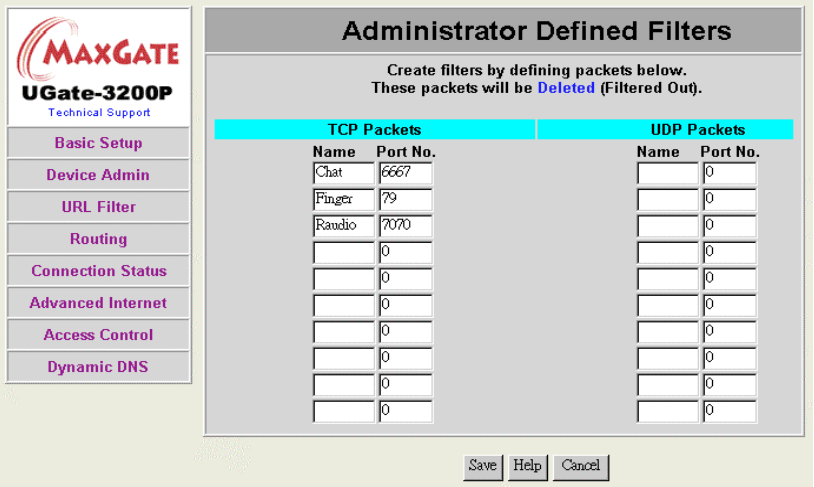
Workstation Data

Workstation Name	Enter a name to identify this workstation.
Network Adapter Address	Hardware address for this workstation. You can use the Windows "Winipcfg" program or your LAN management program to find this address.

Reserve entry in DHCP Table	Check this if you wish to reserve an IP address for this workstation. This is useful if you have to provide the IP Address for other programs or users. If this is left unchecked, the following entry can be ignored.
Reserved IP Address	This relates to the entry above. Enter the reserved address here. This MUST be within the range used by the DHCP server (set on the *Basic Setup* screen).
Security Group	Select the security group for this workstation. If you only wish to reserve an IP Address, and are not using the security (access control) features, simply leave this at "Everyone".

Administrator Defined Filters

The *Filters* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.



Administrator Defined Filters

Create filters by defining packets below.
These packets will be Deleted (Filtered Out).

TCP Packets Name	TCP Packets Port No.	UDP Packets Name	UDP Packets Port No.
Chat	6667		0
Finger	79		0
Raudio	7070		0
	0		0
	0		0
	0		0
	0		0
	0		0
	0		0
	0		0

Figure 30: Filters Screen

This screen allows you to define packet filters. When you define security groups, on the "Security Groups" screen, you can select from any filters defined here, as well as the pre-defined filters.

Data

TCP Packets

Define the packets you wish to be filtered out, by entering the following data.

Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.

UDP Packets

Define the packets you wish to be filtered out, by entering the following data.

Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.

12

Chapter 12

Dynamic DNS:
- Get Your Own Domain

This Chapter explains the benefits and operation of the Dynamic DNS feature.

Overview

Your UGate-3200P is equipped with Dynamic DNS technology.

This technology allows Internet users to connect to Servers on your LAN using a Domain Name rather than an IP Address. The Dynamic DNS feature is particularly useful if you are using the Virtual Server feature. See Chapter 10 for details of using Virtual Servers.

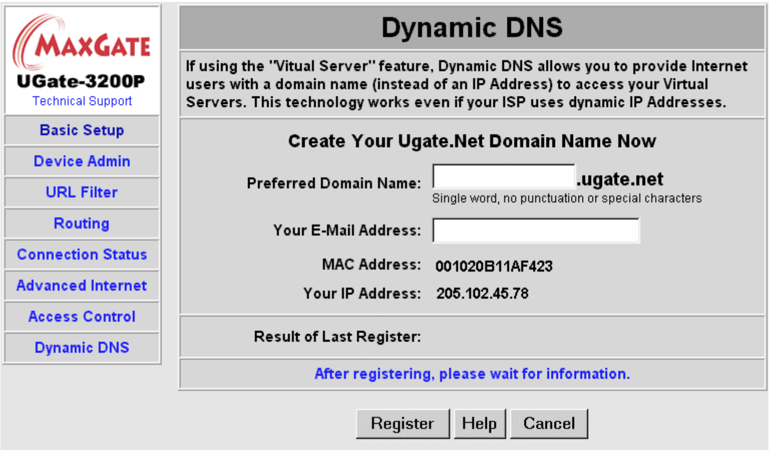
One (1) year of free service is provided, compliments of MaxGate.

To use Dynamic DNS

1. Ensure the UGate-3200P is properly installed and configured, and Internet access is possible.
2. Install and configure the required Server software on PCs on your LAN.
3. Configure the *Virtual Servers* screen of the UGate-3200P with details of the Servers from step 2.
4. Configure the *Dynamic DNS* screen of the Ugate-3200P with the required data on this screen, as described below.
5. Wait for E-Mail confirmation regarding usage of the Domain Name you requested.
6. Once confirmation is received, you can distribute your Domain Name. Internet users can use your Domain name to connect to your Virtual Servers.

   See the “Examples” section later in this Chapter for further details.

Dynamic DNS Screen



Dynamic DNS

If using the "Vitual Server" feature, Dynamic DNS allows you to provide Internet users with a domain name (instead of an IP Address) to access your Virtual Servers. This technology works even if your ISP uses dynamic IP Addresses.

Create Your Ugate.Net Domain Name Now

Preferred Domain Name: ____ .ugate.net
Single word, no punctuation or special characters

Your E-Mail Address: ____

MAC Address: 001020B11AF423

Your IP Address: 205.102.45.78

Result of Last Register:

After registering, please wait for information.

Figure 31: Dynamic DNS

Data – Dynamic DNS

Preferred Domain Name	Enter the domain name you wish to use. You can only apply for domain names in the format `xxxx.ugate.net`
Your E-Mail Address	Enter your email address here for contact information.
Hardware Address	This is the Hardware Address of the Ugate-3200P, as seen on the WAN (Internet) interface.
IP Address	IP Address allocated by your ISP. If not using Dynamic DNS, Internet users would have to use this IP Address to connect to your Virtual Servers. By using Dynamic DNS, Internet users can connect using your Domain Name instead of this IP Address.
Register Button	After entering the data above, use this button to connect to the DDNS Server. You must wait for confirmation before using the Domain Name your requested.

Examples

Running your own Web Server

Running your own WEB server can have its advantages. You can give out your own web site address such as Yourname.Ugate.net! Having control of your own webserver means you can set up and configure the server to your liking, log into your server and get YOUR Website!, Now you don't need to use the web hosting services that is costing you Much More per month! To download Web Server software, go to www.winfiles.com or www.tucows.com.

Procedure

1. Make sure you are connected to the Internet, and obtain your Domain Name using the *Dynamic DNS* screen.
2. Install and configure the Web Server software on a PC on your LAN.
3. Record the IP Address of this PC. (This PC should have a fixed IP Address. Alternatively, you can use the UGate-3200P's DHCP Server but reserve an IP Address for this PC using the *Workstations* screen.)
4. Configure the *Virtual Server* screen on your UGate-3200P.
   - Enable the "Web Server" setting.
   - Enter the IP Address of the PC from step 3.
5. Test using any PC on your LAN. Try to connect by entering the following in the *Address* bar of your Web Browser:

   `www.my_domain.ugate.net`

   Where my_`domain` is the Domain Name you registered.

   If this fails, check that the Web Server is working correctly by connecting directly to it (using its LAN IP Address) from another PC on your LAN.

Note:

The standard port number for Web Servers is 80. If you wish to use a non-standard port number, you need to define a *User-defined Virtual Server*. Also, clients must specify the port number when they try to establish a connection.

Running your own Mail Server

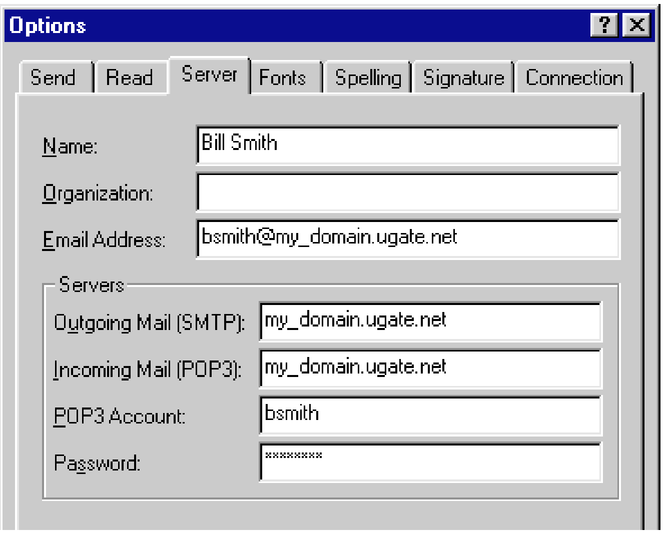
Running your own Mail server can have its advantages. You can give out your own email accounts like yourname@yourname.ugate.net! Having control of your own mail server means you can set up and configure the server to your liking, log into your server and get YOUR email!, Now you can give out email boxes to all your friends and family.

In a business environment, Dynamic DNS allows you to use your own E-Mail Server for both internal and external E-Mail.

To download E-Mail Server software, go to www.winfiles.com or www.Tucows.com. Make sure the software provides both POP3 (mailbox) and SMTP (mail routing) capabilities.

Procedure

1. Make sure you are connected to the Internet, and obtain your Domain Name using the *Dynamic DNS* screen.
2. Install and configure the Mail Server software on a PC on your LAN. You need to create a Mail Account for each user.
3. Record the IP Address of this PC. (This PC should have a fixed IP Address. Alternatively, you can use the UGate-3200P's DHCP Server but reserve an IP Address for this PC using the *Workstations* screen.)
4. Configure the *Virtual Server* screen on your UGate-3200P.
   - Enable both the "Mail (SMTP)" and "Mail (POP3)"settings.
   - For both, enter the IP Address of the PC from step 3.
5. Configure PCs on your LAN to use your E-Mail Server:
   - Start your E-Mail program,
   - Locate the settings for "POP3 Server" and "SMTP Server". For both of these, enter your domain name as shown below (where `my_domain` is the Domain Name you registered).



Name: Bill Smith

Organization:

Email Address: bsmith@my_domain.ugate.net

Outgoing Mail (SMTP): my_domain.ugate.net

Incoming Mail (POP3): my_domain.ugate.net

POP3 Account: bsmith

Password: ********

Figure 32: E-Mail Client Configuration

  - For the “POP3 Account”, enter the user name you defined in your Mail Server program.
  - For the “Password”, enter the password you defined in your Mail Server program.
6. You should now be able to send and receive E-Mail using this account, whether you are connected to your LAN, or connected via the Internet. You can test by sending an E-Mail to yourself.
7. Advise people of your new E-Mail address.
(`bsmith@my_domain.ugate.net` in the example above)

Notes:

- Using this configuration, local E-Mail (sent to other LAN users) will also be routed through the Internet.
If this is undesirable, use your E-Mail client program to create another mail account. Enter the same account name and password, but use the LAN IP Address of your Mail Server for the POP3 and SMTP Server. Your PC will then connect directly to your Mail Server. However, you can only use this account while connected to the LAN.
- If the system does not work, check that your E-Mail Server is configured correctly. You can test your E-Mail Server by setting up an Account as described above, where your PC will connect directly to the Mail Server without using DDNS.
- The standard port numbers for SMTP and POP3 Servers are 25 and 110 respectively. If you wish to use non-standard port numbers, you need to define a *User-defined Virtual Server* and re-configure your E-Mail client program.

Running your own FTP Server

Running your own FTP server can have its advantages. You can give out FTP accounts to your liking, log into your FTP server and get YOUR files from YOUR server, and don't need to use the ISP's FTP server anymore, you have YOURS! Now you can give out access to your FTP site to all your friends and family.

To download FTP Server software, go to www.winfiles.com or www.tucows.com.

Procedure

1. Make sure you are connected to the Internet, and obtain your Domain Name using the *Dynamic DNS* screen.
2. Install and configure the FTP Server software on a PC on your LAN.
3. Record the IP Address of this PC. (This PC should have a fixed IP Address. Alternatively, you can use the UGate-3200P’s DHCP Server but reserve an IP Address for this PC using the *Workstations* screen.)
4. Configure the *Virtual Server* screen on your UGate-3200P.
    - Enable the “FTP Server” setting.
    - Enter the IP Address of the PC from step 3.
5. Test using any PC on your LAN. Try to connect by entering the following in the *Address* bar of your Web Browser:

    ```
    ftp://my_domain.ugate.net
    ```

    Where `my_domain` is the Domain Name you registered.

Note:

Using standard port numbers is strongly recommended. Using non-standard port numbers is very awkward, because FTP servers use 2 port numbers. Also, most Web Browsers do not support non-standard port numbers on the FTP protocol.

Running your own Internet Game Server

Running your own Internet Game Server is fun! You can give out Yourname.Ugate.net and your friends can use that name to connect to your game server. You can forget about what IP address you are using, forget about emailing your IP to all your gaming buddies, and they can now connect directly to yourname.ugate.net

The ugate.net Dynamic DNS service works with most popular TCP/IP Internet Games. Please make sure you check with the gaming manual to enable the proper ports in the UGate-3200P.

Procedure

1. Make sure you are connected to the Internet, and obtain your Domain Name using the *Dynamic DNS* screen.
2. Install and configure the Games Server software on a PC on your LAN.
3. Record the IP Address of this PC. (This PC should have a fixed IP Address. Alternatively, you can use the UGate-3200P's DHCP Server but reserve an IP Address for this PC using the *Workstations* screen.)
4. Configure the *User-Defined Virtual Server* screen on your UGate-3200P with details of the Game Server.
   - Check the Game Server documentation for the "Protocol" and "Port" settings.
   - Enter the IP Address of the PC from step 3.
5. Use the appropriate client software to connect to the Game Server. Specify the Game Server's address as:

```
my_domain.ugate.net
```

Where `my_domain` is the Domain Name you registered.

Using your Ugate.net name with other Internet products

Ugate.net Dynamic DNS is also great for programs like Internet Phone, NetMeeting, CU-Seeme and other video conferencing/Internet phone related products. You can now give out yourname.ugate.net instead of an ever-changing IP address! When friends, family or other Internet users want to connect to a PC on your local LAN to conference with you, they simply have to connect using Yourname.ugate.net

Procedure

1. Make sure you are connected to the Internet, and obtain your Domain Name using the *Dynamic DNS* screen.
2. Install and configure the required software on a PC on your LAN.
3. Record the IP Address of this PC. (This PC should have a fixed IP Address. Alternatively, you can use the UGate-3200P's DHCP Server but reserve an IP Address for this PC using the *Workstations* screen.)
4. Configure the UGate-3200P
    - You can use the *Virtual Server*, *User-defined Virtual Servers*, or *DMZ* feature, as appropriate.
    - Each of these option require you to enter the IP Address of the PC from step 3.
5. Use the appropriate client software to establish a connection. Specify the remote address as:

    `my_domain.ugate.net`

    Where `my_domain` is the Domain Name you registered.

Note:

If using the DMZ feature, it may not be possible to test the connection using another PC on your LAN. You should test using a PC whose Internet connection does not go through the UGate-3200P.

Appendix A

Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the Ugate-3200P and some possible solutions to them. If you follow the suggested steps and the UGate-3200P still does not function properly, contact technical support for further advice.

General Problems

Problem 1: Can’t connect to the UGate-3200P to configure it.

Solution 1: Check the following:

- The UGate-3200P is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the UGate-3200P are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure that your PC is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the UGate-3200P's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the UGate-3200P.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your workstations IP settings are correct (IP address, Network Mask, Default gateway and DNS).
- If the PCs are configured correctly, but still not working, check the UGate-3200P. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the UGate-3200P is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: Some applications do not run properly when using the UGate-3200P.

Solution 2: The UGate-3200P processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications that do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.
- When the *DMZ* feature is being used, the *Special Applications* and *Virtual Server* features should be disabled.

Appendix B

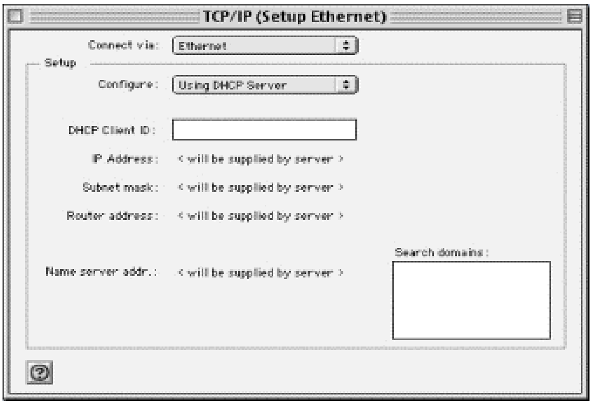
TCP/IP Configuration for Macintosh®

Note: If you currently use a static IP address, write down the existing IP settings including the IP address, Subnet Mask, Router address, and Name Server address before making any of the changes indicated below.

Using the DHCP Server to Assign IP Addresses

1. Click the Apple icon in the upper left corner of the screen and select Control Panel/TCP/IP. The TCP/IP properties dialog box will appear as shown in Figure 33: Using DHCP Server.

.



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Figure 33: Using DHCP Server

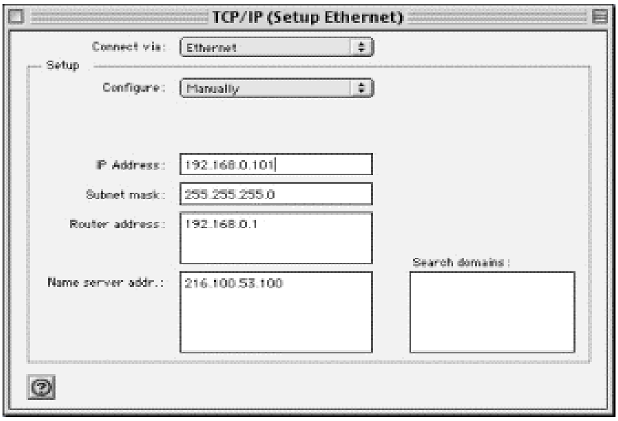
2. From the Connect Via list box, choose Ethernet.
3. From the Configure list box, choose Using DHCP Server
4. Leave the DHCP Client ID field blank.

Manual Assignment of IP Addresses

***Note**: If you have more than one Macintosh, please use different IP addresses on each computer. The IP address range can be from 192.168.0.52 to 192.168.0.254. (See Table 13: IP Addresses and DHCP below.)*

---

1. Click the Apple icon in upper left corner of the screen and select Control Panel/TCP/IP. The TCP/IP properties dialog box will appear as shown in Figure 34: Manual configuration of IP Address.



TCP/IP (Setup Ethernet)

Connect via: Ethernet

Setup

Configure: Manually

IP Address: 192.168.0.101

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Name server addr.: 216.100.53.100

Search domains:

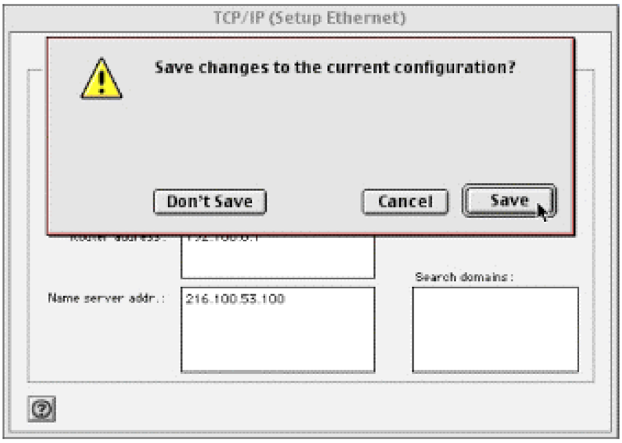
Figure 34: Manual Configuration of IP Addresses

2. In the IP Address field, type an IP address according to the DHCP server status in the table below:

	DHCP server status	
	Enabled	Disabled
IP Address Range	192.168.0.52 to 192.168.0.254	192.168.0.2 to 192.168.0.254

Table 13: IP Addresses and DHCP

3. In the Subnet mask field, type 255.255.255.0
4. In the Router address field, type 192.168.0.1
5. In the Name server addr. Field, type the name server address(es) provided by your ISP.
6. Close this screen and save the configuration as shown in Figure 35: Saving the Configuration.



Save changes to the current configuration?

Name server addr.: 216.100.53.100

Search domains:

Figure 35: Saving the Configuration

7. Restart your computer

***Remember**: You must physically attach the MaxGate device and cable/DSL modem together. For how to put them together, please refer to the main manual.*

Appendix C

Specifications

Model No.:	3200P
Dimensions	9.8in(L) / 8in(W) / 1.4in(H) 250mm(L) / 203mm(D) / 35mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	9 Ethernet: 7 * 10/100Mbps (RJ45) auto-switching hub ports for LAN devices 1 * 10/100Mbps (RJ45) "uplink" port 1 * 10Mbps (RJ45) for WAN port
Printer Port	1 * parallel printer port
LEDs	20
External Power Adapter	9 V DC, 1.5A